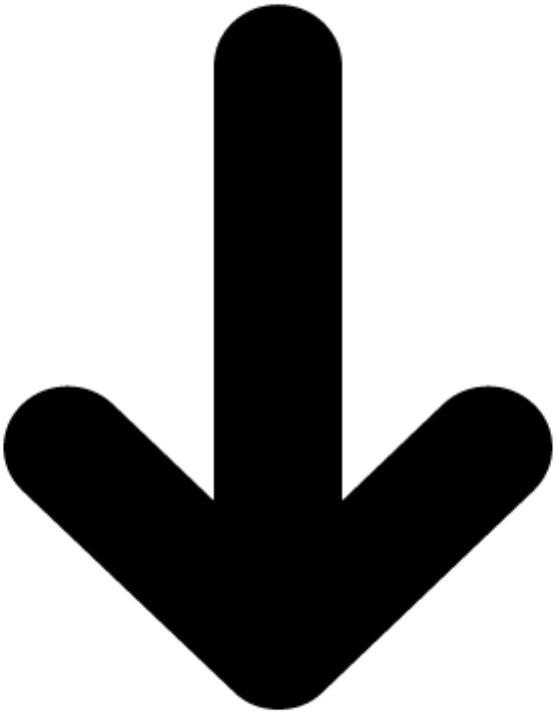
Proyek 6: Implementasi IDS (Intrusion Detection System) dengan Snort / Suricata

Nama Kelompok :

- 2201020098 Muhammad Rifqi
- 2201020123 Handicap
- 2201020139 Muhammad Iqbal Hordani
- 2201020101 Irsyad Widiansyah



Tahapan 3: Simulasi port scanning dengan nmap

- ## Port Scanning

  Port scanning adalah teknik untuk memeriksa port-port yang terbuka pada suatu host atau server.
  Tujuan scanning ini adalah untuk:

  - mengidentifikasi layanan (service) yang berjalan,
  - mengetahui port mana yang terbuka atau tertutup,
  - memetakan potensi celah keamanan pada sistem.

  Dalam konteks keamanan jaringan, port scan merupakan aktivitas yang sering dilakukan oleh penyerang (attacker) untuk mengumpulkan informasi sebelum melakukan serangan lebih lanjut. Oleh karena itu, Intrusion Detection System (IDS) seperti Suricata harus mampu mendeteksi pola scanning tersebut.

- ## Nmap

  Nmap adalah singkatan dari **Network Mapper**, yaitu alat pemindai jaringan berbasis **opensource** yang digunakan untuk menemukan perangkat, port terbuka, dan layanan yang berjalan dalam suatu jaringan komputer. Nmap berfungsi untuk eksplorasi jaring an dan audit keamanan, serta membantu dalam mengidentifikasi potensi kerentanan d alam sistem jaringan. Alat ini sangat populer di kalangan profesional keamanan infor masi dan digunakan untuk berbagai tujuan, termasuk pemetaan jaringan dan pengujia n penetrasi.

- ## Tujuan Simulasi

  1. Menghasilkan aktivitas port scanning dari mesin attacker menggunakan Nmap
  2. Memvalidasi apakah Suricata dapat mendeteksi pola scan tersebut
  3. Menghasilkan log yang dapat dianalisis pada tahap selanjutnya

  Dengan melakukan simulasi ini, mahasiswa dapat memahami bagaimana IDS mendeteksi pola scanning melalui rule bawaan Suricata.

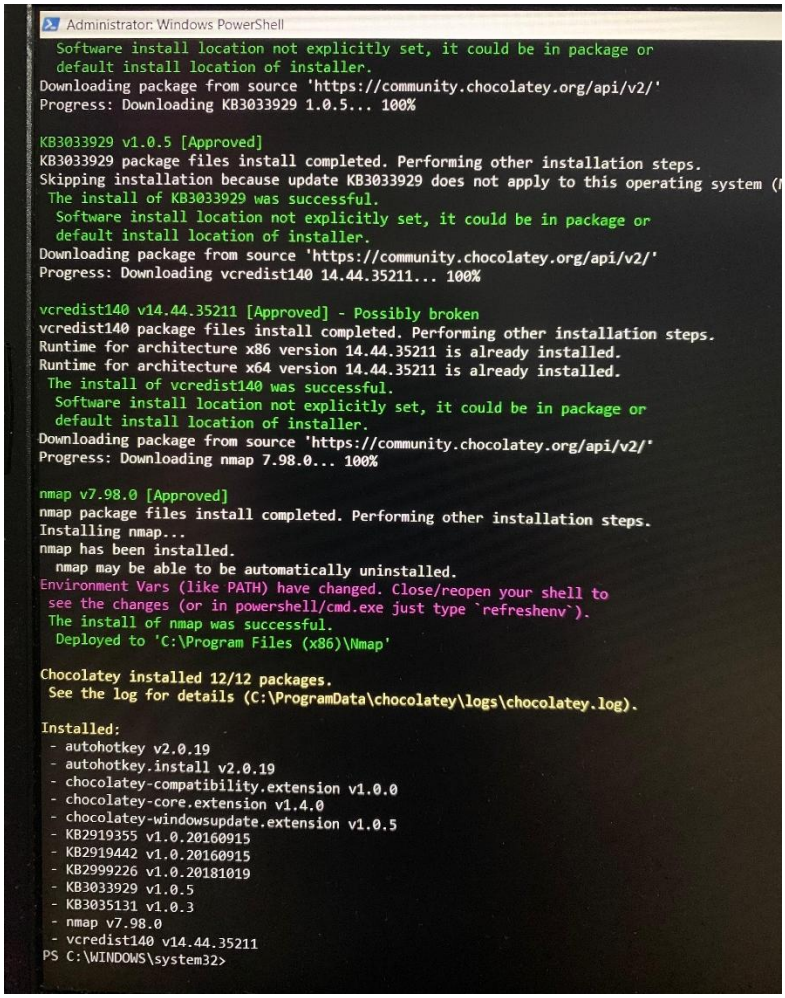
- ## Membagi 2 mesin

  1. **Mesin 1 = Attacker (** Memiliki Nmap dan akan melakukan scanning.)
  2. **Mesin 2 = Victim** (Menjalankan Suricata dan menjadi target scanning.)

     Catatan *

Proggres Mesin 1 = Attacker menggunakan

1. Install Nmap
    - choco install nmap -



    - cek instalasi Nmap : nmap -v

```
PS C:\Users\Handicap> nmap -v
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-04 12:55 +0700
Read data files from: C:\Program Files (x86)\Nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.23 seconds
           Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
```

2. Simulasi Port Scanning dengan Nmap, Ip target = 192.168.56.102
    - Normal scan

      Normal scan adalah metode scanning standar Nmap yang digunakan untuk memeriksa port mana saja yang terbuka pada target.
      Scan ini mengirimkan paket TCP ke beberapa port umum dan menampilkan status port seperti **open**, **closed**, atau **filtered**.
      Perintah : nmap <IP_Target>

```
PS C:\Users\Handicap> nmap 192.168.56.102
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-04 13:58 +0700
Nmap scan report for 192.168.56.102 (192.168.56.102)
Host is up (0.0012s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:F3:C1:37 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
PS C:\Users\Handicap>
```

      Output :

      • **Target IP:** 192.168.56.102
      • **Host Status:** Up
      • **Port Terbuka:**

        - **22/tcp – SSH**
          • **MAC Address:** 08:00:27:F3:C1:37 (VirtualBox NIC)
          • **Jumlah Port Tertutup:** 999 port closed
          • **Waktu Scan:** ~0.26 detik

    - SYN scan (Stealth Scan)

      SYN scan adalah jenis scanning yang hanya mengirim paket **SYN** tanpa menyelesaikan proses handshake TCP.Teknik ini sering digunakan penyerang karena lebih cepat, lebih “diam-diam”, dan sering tidak tercatat oleh service target.IDS seperti Suricata biasanya mendeteksi scan ini sebagai aktivitas mencurigakan.
      Perintah : sudo nmap -sS <IP_Target>

```
PS C:\Users\Handicap> nmap -sS 192.168.56.102
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-04 14:05 +0700
Nmap scan report for 192.168.56.102 (192.168.56.102)
Host is up (0.0017s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:F3:C1:37 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

Output :

- **Target IP:** 192.168.56.102
- **Host Status:** Up
- **Port Terbuka:**
  - **22/tcp – SSH**
    - **MAC Address:** 08:00:27:F3:C1:37 (VirtualBox NIC)
    - **Jumlah Port Tertutup:** 999 port closed
    - **Network Distance:** 1 hop (VM lokal)
    - **Waktu Scan:** ~0.23 detik

- Aggressive scan (-A Scan)

  Aggressive scan melakukan scanning yang lebih lengkap:
  - mendeteksi versi service
  - identifikasi sistem operasi (OS detection)
  - melakukan traceroute
  - scanning port secara menyeluruh

  Metode ini menghasilkan traffic lebih banyak dan mudah terdeteksi oleh IDS.

  Perintah : sudo nmap -A <IP_Target>

```
PS C:\Users\Handicap> nmap -A 192.168.56.102
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-04 14:06 +0700
Nmap scan report for 192.168.56.102 (192.168.56.102)
Host is up (0.0013s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 c4:4c:c7:1d:ba:9c:c7:fb:d6:a4:2f:0e:85:08:06:9c (ECDSA)
|_  256 f3:b9:a4:4c:bb:af:9d:97:0f:03:ae:21:69:e9:43:6f (ED25519)
MAC Address: 08:00:27:F3:C1:37 (Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6
.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.26 ms 192.168.56.102 (192.168.56.102)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.83 seconds
PS C:\Users\Handicap>
```

Output :

- Target IP: 192.168.56.102
- Host Status: Up
- Port Terbuka:
    - 22/tcp – OpenSSH 9.6p1 (Ubuntu 3ubuntu13.14)
- SSH Host Key:
    - Fingerprint ECDSA & ED25519 terdeteksi
- OS Detection:
    - Teridentifikasi sebagai Linux (kernel 4.x – 5.x)
- Device Type:
    - General purpose / router-like (VirtualBox VM)
- Network Distance: 1 hop (satu jaringan / host-only)
- Waktu Scan: ~6.83 detiK

3. HASIL SCANNING OLEH MESIN 2 (IDS DENGAN SURICATA)
    - Scaning dari server attacker Nmap 192.168.56.102 dan Nmap -Ss 192.168.56.102

```
ubuntu@ubuntuserver:~$ sudo tail -f /var/log/suricata/fast.log
12/04/2025-07:05:40.299555  [**] [1:1000003:1] ET SCAN Potential SYN Scan [**] [Classification: (null)] [Priority: 3] {T
CP} 192.168.56.1:63473 -> 192.168.56.102:139
12/04/2025-07:05:54.379186  [**] [1:1000003:1] ET SCAN Potential SYN Scan [**] [Classification: (null)] [Priority: 3] {T
CP} 192.168.56.1:62012 -> 192.168.56.102:554
```

Output:

• **Alert Terdeteksi:** ET SCAN Potential SYN Scan
• **Jenis Aktivitas:** Suricata mendeteksi percobaan **SYN Scan** (teknik yang digunakan oleh nmap -sS).
• **Sumber Trafik:**

- **192.168.56.1** (host Windows kamu) → **192.168.56.102** (server Ubuntu)
  • **Port Tujuan:** Port acak (139, 554, dan lainnya) karena proses scanning.
  • **Prioritas Alert:** 3 (Moderate)

    - Scaning dari server attacker Nmap -A 192.168.56.102

```
12/04/2025-07:06:53.102356  [**] [1:1000002:1] ET SCAN Nmap Scripting Engine Scan [**] [Classification: (null)] [Priorit
y: 3] {TCP} 192.168.56.1:47065 -> 192.168.56.102:22
12/04/2025-07:06:53.103100  [**] [1:1000002:1] ET SCAN Nmap Scripting Engine Scan [**] [Classification: (null)] [Priorit
y: 3] {TCP} 192.168.56.1:47066 -> 192.168.56.102:22
12/04/2025-07:06:53.398259  [**] [1:1000002:1] ET SCAN Nmap Scripting Engine Scan [**] [Classification: (null)] [Priorit
y: 3] {TCP} 192.168.56.1:47067 -> 192.168.56.102:22
12/04/2025-07:06:53.653288  [**] [1:1000002:1] ET SCAN Nmap Scripting Engine Scan [**] [Classification: (null)] [Priorit
y: 3] {TCP} 192.168.56.1:47068 -> 192.168.56.102:22
12/04/2025-07:06:53.901165  [**] [1:1000002:1] ET SCAN Nmap Scripting Engine Scan [**] [Classification: (null)] [Priorit
y: 3] {TCP} 192.168.56.1:47069 -> 192.168.56.102:22
12/04/2025-07:06:54.128868  [**] [1:1000001:1] ET SCAN Nmap OS Detection Probe [**] [Classification: (null)] [Priority:
3] {TCP} 192.168.56.1:47069 -> 192.168.56.102:22
12/04/2025-07:06:54.279006  [**] [1:1000002:1] ET SCAN Nmap Scripting Engine Scan [**] [Classification: (null)] [Priorit
y: 3] {TCP} 192.168.56.1:47070 -> 192.168.56.102:22
12/04/2025-07:06:54.524046  [**] [1:1000002:1] ET SCAN Nmap Scripting Engine Scan [**] [Classification: (null)] [Priorit
y: 3] {TCP} 192.168.56.1:47071 -> 192.168.56.102:22
12/04/2025-07:06:54.778949  [**] [1:1000002:1] ET SCAN Nmap Scripting Engine Scan [**] [Classification: (null)] [Priorit
y: 3] {TCP} 192.168.56.1:47072 -> 192.168.56.102:22
12/04/2025-07:06:54.999949  [**] [1:1000001:1] ET SCAN Nmap OS Detection Probe [**] [Classification: (null)] [Priority:
3] {TCP} 192.168.56.1:47072 -> 192.168.56.102:22
12/04/2025-07:07:57.891600  [**] [1:1000001:1] ET SCAN Nmap OS Detection Probe [**] [Classification: (null)] [Priority:
3] {TCP} 192.168.56.1:47070 -> 192.168.56.102:22
12/04/2025-07:07:58.840129  [**] [1:1000001:1] ET SCAN Nmap OS Detection Probe [**] [Classification: (null)] [Priority:
3] {TCP} 192.168.56.1:47071 -> 192.168.56.102:22
12/04/2025-07:07:59.894383  [**] [1:1000001:1] ET SCAN Nmap OS Detection Probe [**] [Classification: (null)] [Priority:
3] {TCP} 192.168.56.1:47068 -> 192.168.56.102:22
12/04/2025-07:08:00.890941  [**] [1:1000001:1] ET SCAN Nmap OS Detection Probe [**] [Classification: (null)] [Priority:
3] {TCP} 192.168.56.1:47067 -> 192.168.56.102:22
```

Kesimpulan

Berdasarkan hasil pemindaian menggunakan **Nmap -sS** dan **Nmap -A** terhadap target **192.168.56.102**, Suricata berhasil mendeteksi seluruh aktivitas scanning yang dilakukan dari host **192.168.56.1**. Pada pemindaian **-sS**, Suricata mencatat alert **ET SCAN Potential SYN Scan**, yang menunjukkan bahwa IDS mampu mengenali pola stealth scan (SYN scan) secara efektif.

Sementara itu, pada pemindaian **-A** yang lebih agresif, Suricata mendeteksi aktivitas tambahan berupa **ET SCAN Nmap Scripting Engine Scan** dan **ET SCAN Nmap OS Detection Probe**, yang muncul akibat proses deteksi OS, pemeriksaan layanan, dan eksekusi Nmap Scripting Engine.

Secara keseluruhan, hasil ini menunjukkan bahwa Suricata berfungsi dengan baik sebagai IDS, karena berhasil mengidentifikasi perbedaan jenis scanning—baik yang bersifat stealth maupun agresif—dan memberikan alert yang sesuai terhadap setiap pola serangan yang muncul.